REMARKS

This Amendment is responsive to the Office Action dated December 6, 2007. Applicant has amended claims 1, 6, 40, 41, 43, 49, 69, 70, and 113. Applicant has also cancelled claim 7 and 78-109 and added new claims 123-132. Claims 1-6, 8-77, 110-132 are pending upon entry of this Amendment.

Claim Rejection Under 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 1-77 and 110-122 under 35 U.S.C. §102(e) as being anticipated by Garza (US 2003/0208689). Applicant respectfully traverses the rejection to the extent such rejection may be considered applicable to the amended claims. Garza fails to disclose each and every feature of the claimed invention, as required by 35 U.S.C. §102(e).

Claims 1-42

Applicant's independent claim 1, as amended, is directed to a method comprising receiving, with a forensic device coupled to a target computing device via a communication link, input from a remote user of a client device that identifies computer evidence to acquire from the target computing device. Claim 1, as amended, literally requires acquiring the computer evidence from the target computing device with the forensic device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence. Applicant's claim 1 also recites storing the computer evidence on the forensic device and presenting a user interface for the forensic device through which the remote user views and analyzes, using the client device, the computer evidence acquired from the target computing device.

Garza describes a remote computer forensic evidence collection system.[1] The remote evidence collection system of Garza includes a victim machine and a secure evidence aggregation server.[2] Operation of the remote evidence collection system of Garza is described in

[1] Garza, ¶ [0010].
[2] Id. at ¶¶ [0013]-[0014].

paragraphs [0022]-[0033]. In operation, an incident response team receives information about a victim machine for which a security incident has occurred and generates a kernel boot image, i.e., software, for the victim machine using the information provided.[3] The victim machine is then rebooted with the kernel boot image.[4] In other words, the victim machine is shut down and restarted using the kernel boot image. Forensic computer evidence, e.g., in the form of a copy of the rebooted victim machine, is generated and streamed to the evidence aggregation server via an SSL connection.[5] When the victim machine of Garza is rebooted with the kernel boot image, current state information such as running processes, open network connections, memory (process memory and physical memory) are lost. Thus, the information generated and streamed to the evidence aggregation server via the SSL connection is only disk-based data. After the copy of the drive of the victim machine has successfully completed, the drive on the evidence aggregation server is removed and remitted to a chain of custody.

First, Garza fails to disclose receiving, with a forensic computing device, input from a remote user of a client device that identifies computer evidence to acquire from a target computing device and acquiring the computer evidence from the target computing device with the forensic device coupled to the target computing device via a communication link, as recited in Applicant's claim 1. Thus, Applicant's claim 1 requires three separate computing devices; (1) a target computing device, (2) a forensic device; and (3) a remote client device. As described above, Garza describes an evidence aggregation system that includes only two computing devices, i.e., the victim machine and the evidence aggregation server.

Second, Garza also fails to teach or suggest acquiring the computer evidence from the target computing device with the forensic device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence, as recited in Applicant's claim 1. To the contrary, Garza describes loading acquisition software (i.e., the kernel boot image) on the victim machine prior to acquiring the computer evidence.[6] In particular, disk imaging

[3] Id. at ¶¶ [0022]-[0027].
[4] Id. at ¶ [0029].
[5] Id. at ¶ [0031].
[6] Id. at ¶ [0029].

software, such as a Unix copy command dd, included in the kernel boot image loaded onto the victim machine generates the forensic computer evidence.[7]

For at least these reasons, Garza fails to disclose the requirements of Applicant's independent claim 1. Moreover, Garza fails to disclose a number of the features of Applicant's dependent claims 2-42. For example, Garza fails to disclose acquiring state information from the target computing device that includes at least one of running process information and open network ports with associated processes, as recited in Applicant's dependent claim 6. As described above, the victim machine in Garza is rebooted with the kernel boot image. When the victim machine is rebooted, at least a portion of the state information of the victim machine is lost. In particular, running process information as well as open network connections and associated processes are lost upon rebooting of the victim machine. Thus, the evidence acquisition system described in Garza is unable to obtain state information that includes running process information or open network connections and associated processes, as required by Applicant's claim 6.

As another example, Garza fails to disclose performing a subset of the acquisition operations to acquire at least one of a log file and communication statistics prior to performing the other acquisition operations, as recited in Applicant's claim 13. Garza describes the kernel boot image loaded onto the victim machine taking a bit by bit image of the victim machine.[8] Garza fails to describe any order in which acquisition operations are performed during the taking of the bit by bit image of the victim machine. Therefore, Garza could not possibly anticipate performing a subset of the acquisition operations to acquire first at least one of a log file and communication statistics prior to performing the other acquisition operations, as recited in Applicant's claim 13. In fact, Garza fails to make any mention whatsoever of a log file or communication statistics of the victim machine.

As another example, Garza fails to disclose the forensic device being coupled to the target computing device via a customer network of the target computing device, as recited in Applicant's claim 40, as amended. The forensic device of Garza is not coupled to the target computing device via a customer network of the target computing device. Instead, the evidence

[7] Id. at ¶ [0041].
[8] Garza, ¶ [0049].

aggregation server of Garza is coupled to the victim machine via a public network (e.g., Internet) and communicates with the victim machine over the Internet using an SSL connection.[9]

For at least these reasons, Garza fails to disclose the features of Applicant's claims 1-42. Applicant therefore respectfully requests withdrawal of the rejection.

Claims 43-70 and 113-122

Applicant's independent claim 43 recites a system comprising a target computing device, a forensic device coupled to the target computing device via a customer network of the target computing device, a client device and a user interface module to present a user interface for the forensic device that is remotely accessible by the client device. Applicant's independent claim 43 further recites that the forensic device receives input via the user interface that identifies computer evidence to acquire from a target computing device and, in response, acquires the computer evidence from the target computing device, stores the computer evidence, and presents the computer evidence to the remote user for analysis via the user interface.

Applicant's independent claim 113 recites a computer-readable medium comprising instructions that cause a processor to receive, with a forensic device coupled to a target computing device via a customer network of the target computing device, input from a remote user of a client device that identifies computer evidence to acquire from the target computing device, acquire the computer evidence from the target computing device with the forensic device, store the computer evidence on the forensic device, and present a user interface for the forensic device through which the remote user views and analyzes, with the client device, the computer evidence acquired from the target computing device.

Garza fails to disclose the requirements of Applicant's claims 43 and 113. Garza fails to disclose a target computing device, a forensic device coupled to a customer network of the target computing device, and a client device that remotely accesses the forensic device, as recited in Applicant's claims 43 and 113. As described above with respect to Applicant's claim 1, Garza describes an evidence aggregation system that includes only two computing devices, i.e., the victim machine and the evidence aggregation server. Additionally, the forensic device of Garza

[9] Garza, ¶ [0040].

is not coupled to the target computing device via a customer network of the target computing device. Instead, the evidence aggregation server of Garza is coupled to the victim machine via a public network (e.g., Internet) and communicates with the victim machine over the Internet using an SSL connection.[10]

For at least these reasons, Garza fails to disclose the requirements of Applicant's claims 43-70 and 113-122. Applicant respectfully requests withdrawal of the rejection.

Claims 71-77

Applicant's independent claim 71 comprises a method to remotely acquire computer forensic evidence comprising receiving input from a remote user that identifies computer evidence to be acquired from a target computing device, determining an order in which to perform acquisition operations to acquire the computer evidence from the target computing device with reduced impact on other data stored on the target computing device, wherein acquisition operations to acquire at least one of an log file and communication statistics occur in the order prior to any other acquisition operations and communicating commands to initiate the acquisition operations on the target computing device in accordance with the determined order. Garza fails to disclose the requirements of Applicant's claim 71.

As an example, Garza fails to disclose determining an order in which to perform acquisition operations to acquire the computer evidence from the target computing device with reduced impact on other data stored on the target computing device, wherein acquisition operations to acquire at least one of a log file and communication statistics occur in the order prior to any other acquisition operations. Garza describes the kernel boot image loaded onto the victim machine taking a bit by bit image of the victim machine.[11] Garza fails to describe any order in which acquisition operations are performed during the taking of the bit by bit image of the victim machine. Therefore, Garza could not possibly anticipate ordering acquisition operations such that acquisition operations to acquire at least one of a log file and communication statistics occur in the order prior to any other acquisition operations, as recited in

[10] Garza, ¶ [0040].
[11] Garza, ¶ [0049].

Applicant's claim 71. In fact, Garza fails to make any mention whatsoever of a log file or communication statistics of the victim machine.

For at least these reasons, Garza fails to disclose the features of Applicant's claims 71-77. Applicant respectfully requests withdrawal of this rejection.

Claims 110-112

Applicant's independent claim 110, recites a forensic analysis device that is adapted to operate as an intermediate device between a target computing device and a client device associated with a remote forensic investigator, wherein the analysis device comprises an acquisition module to acquire state information from the target computing device and store the state information on the forensic device while the target device remains active.

The evidence aggregation server of Garza is not adapted to operate as an intermediate device between a target computing device and a client device associated with a remote forensic investigator. To the contrary, the evidence aggregation server of Garza is the device associated with the remote forensic investigator. As describe above with respect to claim 1, the remote forensic investigator inputs data associated with the victim machine into a CGI template of the evidence aggregation server, which then generates an appropriate kernel boot image for the victim machine.[12] The victim machine, operating in accordance with the boot image, directly transfers data to the evidence aggregation server for storage.[13] Thus, the evidence aggregation server of Garza does not operate as the intermediate device between the target computing device and a client device associated with a remote forensic investigator, as recited in Applicant's claim 110. Applicant respectfully requests withdrawal of this rejection.

New Claims

Applicant has added claims 123-132 to the pending application. The Garza fails to disclose the inventions defined by Applicant's new claims. For example, Garza fails to disclose acquiring the computer evidence from the target computing device without the target computing device being shut down, as recited in Applicant's claim 124. As described with respect to claim

[12] Garza, ¶ [0027].
[13] Garza, ¶ [0031].

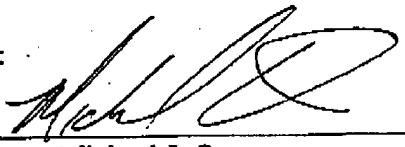
1, the victim machine of Garza is shut down to reboot the victim machine with the kernel boot image. As another example, Garza fails to disclose obtaining an image of a memory of the target computing device, as recited in Applicant's claim 126. As described above, data and information stored in the memory (e.g., process information and state data) of the victim machine of Garza is lost when the victim machine is rebooted with the kernel boot image. Thus, the evidence aggregation server is unable to obtain an image of a memory of the target computing device, as required by Applicant's claim 126. No new matter has been added by way of the new claims.

CONCLUSION

In the foregoing remarks, Applicant has focused on the requirements of the independent claims for purposes of conciseness. In so doing, Applicant in no way admits or acquiesces in the propriety of the Office Action in regard to interpretation of the prior art or any of the additional limitations set forth in the various claims, including the limitations of the dependent claims.

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date: 3-6-08

By: 

Name: Michael J. Ostrom
Reg. No.: 58,730

SHUMAKER & SIEFFERT, P.A.
1625 Radio Drive, Suite 300
Woodbury, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102